REMARKS

Claims 7-18 are pending in this application. By this Amendment, claims 1-6 are canceled; and new claim 7-18 are added.

No new matter is added to the application by this Amendment. Support for new claims 7-18 can be found in canceled claims 1-6, within Figs. 1 and 2, as originally filed, and within the specification, as originally filed, at, for example, paragraphs [0007]-[0010], [0014]-[0017], [0019] and [0021] of US Patent Publication No. 2006/0253774 for the present application.

Reconsideration of the application is respectfully requested.

I. Rejection Under 35 USC 112

Claims 1-6 were rejected under 35 USC 112, second paragraph, as allegedly being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicants regard as the invention. This claim rejection is respectfully traversed.

In view of the cancelation of claims 1-6, this rejection is moot.

Accordingly, withdrawal of the rejection to the claims is respectfully requested.

II. New Claims 7-18

Applicants take this opportunity to submit that new claims 7-18 are not taught or suggested by US Patent No. 5,594,796 to Grube et al. (hereinafter "Grube").

New independent claims 7 and 9 require a gate device configured to (a) perform

a file-selective check for access possibilities to a file outside the local network by checking the file sent from the local network to the connection for presence of a security tag before the file is sent to the external network via the at least one communication channel, and (b) block the sending of the file to the external network if the security tag is found to be present in the file.

Additionally, new independent claim 8 requires a method having the steps of (a) performing a file-selective check for access possibilities to the file outside the local network domain via the gate device checking the file sent from the local network domain for presence of a security tag before the file is sent to the external network via the at least one communication channel, and (b) blocking the sending of the file to the external network if the security tag is found to be present in the file.

Moreover, new independent claim 18 requires a gate device configured to (a) perform a file-selective check for access possibilities to a file outside the local network by checking the file sent from the local network to the connection for presence of a security tag before the file is sent to the external network via the at least one communication channel, and (b) send the file to the external network if the security tag is only found to be present in the file.

Grube discloses a technique to prevent pirates from distributing copyrighted information from illegal databases over a wireless network. Grube's security tags are used in the data, which can be uniquely linked to authorized distributors. A gateway between a database and a wireless network tests data for the presence of these

security tags and compares the security tags with the identity of the actual distributor, to determine whether the data has been sent by an authorized distributor.

Thus, Grube fails to teach or suggest gate device configured to perform and a step of performing a file-selective check for access possibilities to a file outside the local network by checking the file sent from the local network to the connection for presence of a security tag before the file is sent to the external network via the at least one communication channel as required by the present claims.

Moreover, Grube also fails to teach or suggest blocking the sending of or sending a file if a security tag is found or not found to be present. Instead, Grube specifically discloses:

> With such a method and apparatus, the unauthorized distribution of data within a wireless communication system ***can be identified*** and ***subsequently prevented***, thereby ***recapturing*** stolen revenues for the owners of the data and the wireless communication system (emphasis added, see col. 2, lines 49-54);
>
> If the identities between the original database and the current database differ, then the current database is ***identified*** as a potential unauthorized distributor of data (emphasis added, see col. 4, lines 5-8);
>
> If the database identifications are not the same, the security gateway automatically takes a predetermined course of action which may be ***identify*** the current database 117 as a potential unauthorized distributor of data, i.e., a pirate database. In this case, the security gateway 103 ***notifies*** the authorized distributor of the data **that was illicitly transmitted** by the pirate database 117 (emphasis added, col. 5, lines 56-62);
>
> If the comparison at step 305 does not match, then the current particular database, i.e., the database ***transferring the data***, is ***flagged*** by the security gateway as an unauthorized distributor in step 306 (emphasis added, see col. 6, lines 42-45); and
>
> ***Subsequent*** data file transfers are monitored for security tags to determine if the data is being distributed by an authorized data distributor. If the security tag reveals that a current data transmission is being executed by an authorized, or pirate, data distributor, the original database ***is notified. Once notified, the authorized data distributors may take appropriate action to prevent additional pirated transmissions and lost revenue*** (emphasis added, see col. 7, lines 6-13).

Thus, at best, Grube discloses use of a security tag to identify unauthorized distribution of data that was illicitly transmitted from a pirate database, which may be flagged by the security gateway. After the unauthorized distribution is identified and the pirate database is tagged, the authorized distributor(s) is notified so that appropriate action to subsequently prevent additional pirated transmission may be taken by the authorized distributor(s). Nowhere does Grube teach or suggest any blocking a data transmission or blocking or sending data transmission based on a presence or absence of a security tag. Instead, Grube teaches that the data transmission is illicitly transmitted regardless of whether the transmission is a pirated transmission or an authorized transmission, and then the authorized distributors is notified and may or may not take subsequent steps to prevent additional subsequent pirated transmissions.

Accordingly, Grube fails to teach or suggest the features specifically required in new independent claims 7-9 and 18. Because the because the specifically defined features of independent claims 7-9 and 18 are neither taught nor suggested by Grube, Grube cannot anticipate, and would not have rendered obvious, the features specifically defined in those claims.

For at least these reasons, claims 7-18 are patentably distinct from and/or non-obvious in view of the teachings of Grube.

III. Conclusion

In view of the foregoing, it is respectfully submitted that this application is in condition for allowance. Favorable reconsideration and prompt allowance of claims 7-18 are earnestly solicited.

Should the Examiner believe that anything further would be desirable in order to place this application in even better condition for allowance, the Examiner is invited to contact the undersigned at the telephone number set forth below.

Early and favorable action is earnestly solicited.

CONDITIONAL PETITION FOR EXTENSION OF TIME

If entry and consideration of the amendments above requires an extension of time, Applicants respectfully request that this be considered a petition therefor. The Commissioner is authorized to charge any fee(s) due in this connection to Deposit Account No. 14-1263.

ADDITIONAL FEE

Please charge any insufficiency of fees, or credit any excess, to Deposit Account No. 14-1263.

Respectfully submitted,

NORRIS MCLAUGHLIN & MARCUS, P.A.

By /Brian C. Anscomb/
Brian C. Anscomb – Reg. 48,641
Attorney for Applicants
875 Third Avenue, 8th Floor
New York, NY 10022
Tel. 212-808-0700